



06-02-04

BPAF
2134

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Serial No. : 09/429,174 Confirmation No. (None)

Appellants : Jung-Chih Huang, et al.

Filed : October 28, 1999

Title : PRE-BOOT SECURITY CONTROLLER

TC/A.U. : 2134

Examiner : Christopher J. Brown

Docket No. : 2139

Customer No.: 23320

RECEIVED

JUN 04 2004

MAIL STOP APPEAL BRIEF - PATENTS

Commissioner for Patents

Post Office Box 1450

Alexandria, Virginia 22313-1450

Technology Center 2100

Sir:

APPEAL BRIEF TRANSMITTAL

Enclosed herewith are three (3) copies of an Appeal Brief for this patent application together with a check in the amount of the small entity fee for filing a brief in support of an appeal.

///

///

///

///

///

///

///

///

///

///

///

///

2



RECEIVED

JUN 04 2004

Technology Center 2100

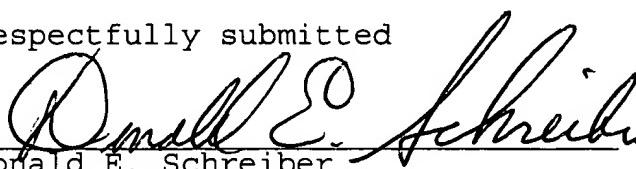
Appeal No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

If any additional fee is required, the Commissioner for Patents is hereby authorized to charge any deficiency or credit any surplus in any relevant fee to Deposit Account No. 19-0735. A duplicate copy of this transmittal letter is enclosed herewith.

Respectfully submitted



Donald E. Schreiber

Reg. No. 29,435

Dated: 1 June, 2004

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Appellants

-2-

Docket no. 2139

June 1, 2004



#18
103

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

EV 380 185 202 US
"Express Mail" mailing Number

1 June, 2004
Date of Deposit

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above addressed to

MAIL STOP AF
Commissioner for Patents
Post Office Box 1450
Alexandria, Virginia 22313-1450

Donald E. Schreiber

Donald E. Schreiber

Dated: 1 June, 2004

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926
(530) 546-6041

Serial No. : 09/429,174 Confirmation No. (None)
Appellants : Jung-Chih Huang, et al.
Filed : October 28, 1999
Title : PRE-BOOT SECURITY CONTROLLER
TC/A.U. : 2134
Examiner : Christopher J. Brown

RECEIVED

Docket No. : 2139
Customer No.: 23320

JUN 04 2004

Technology Center 2100

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
Post Office Box 1450
Alexandria, Virginia 22313-1450

Sir:

APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.192, through his undersigned attorney Appellants submit in triplicate the following brief appealing a rejection of claims that appears in an Office Action mailed on January 14, 2004.

06/03/2004 MAHMED1 00000061 09429174

01 FC:2402

165.00 OP

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

Real Party in Interest

The real party in interest is O₂ Micro International Ltd., a Cayman Island corporation having an office at West Bay Road, P. O. Box 32331 SMB, George Town, Grand Cayman, Cayman Islands, British West Indies.

Related Appeals and Interferences

Appellants are unaware of any presently pending appeal or interference that is related to this appeal.

Status of the Claims

Claims 1-18 are pending in this application, claims 1-18 have been finally rejected, and that rejection of claims is being appealed.

Status of Amendments

The claims were last amended in a response mailed on October 14, 2003, to a first Examiner's Action mailed on July 16, 2003. Pursuant to an Advisory Action mailed on April 20, 2004, claims 1-18 as amended on October 14, 2003, stand finally rejected.

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

Summary of the Invention

The invention, encompassed by the finally rejected claims, resides in an integrated circuit pre-boot security controller that must include a non-volatile password memory for storing at least one user password. A password input circuit, which must also be included in the pre-boot security controller, receives a password for comparison with any user passwords recorded in the password memory. If the pre-boot security controller is operating in a security operating mode, a digital logic circuit, which must also be included in the pre-boot security controller, compares the received password with any user passwords recorded in the password memory. If the password received by the password input circuit matches a user password recorded in the password memory, an output circuit, which must also be included in the pre-boot security controller and that is coupled to the digital logic circuit, transmits an output signal to a power subsystem to enable energizing operation of a device such as a digital computer.

The structure for the integrated circuit pre-boot security controller encompassed by the finally rejected claims inherently securely blocks a thief's attempt to extract password(s) recorded in controller's password memory. Consequently, anyone who steals a digital computer which includes the claimed pre-boot security controller, or without authorization attempts to turn it on and use

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

it, can most practically do so only by physically altering the digital computer, e.g. unsoldering the pre-boot security controller integrated circuit from the computer's motherboard and replacing it with a new integrated circuit for recording new passwords.¹ Thus, for all practical purposes a thief who might consider stealing a device protected by the present invention is truly incapable of using it. Therefore, if a putative thief is aware that the integrated circuit pre-boot security controller protects a device, they will almost certainly be deterred from stealing it.

The Issues

I. Whether, as set forth in the January 14, 2004, Office Action on pages 3 and 4, claims 1, 3, 4, 7, 8, 10, 12, 13, 16 and 17 are obvious under 35 U.S.C. § 103(a) based upon:

A. United States Patent no. 4,604,708 entitled "Electronic Security System for Electronically Powered Devices" that issued on August 5, 1986, on a patent application filed by Gainer R. Lewis ("the Lewis patent"); in view of

¹ Unsoldering an integrated circuit from a digital computer's motherboard and successfully attaching a new one requires a great deal of manual dexterity. Furthermore, someone attempting to alter a digital computer in this way must possess a supply of unused pre-boot security controller integrated circuits which, in general, are only available by buying a new digital computer.

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

B. United States Patent no. 5,251,304 entitled "Integrated Circuit Microcontroller With On-Chip Memory and External Bus Interface and Programmable Mechanism for Securing the Contents of On-Chip Memory" which issued on a patent application filed in the names of James M. Sibigtroth, Michael W. Rhoades, George G. Grimmer, Jr. and Susan W. Longwell ("the Sibigtroth, et al. patent").

II. Whether, as set forth in the January 14, 2004, Office Action on page 5, claims 6 and 15 are obvious under 35 U.S.C. § 103(a) based upon:

A. the Lewis patent; in view of
B. the Sibigtroth, et al. patent; and further in view of
C. United States Patent no. 5,313,639 entitled "Computer With Security Device for Controlling Access Thereto" which issued May 17, 1994, on a patent application filed by George Chao ("the Chao patent").

III. Whether, as set forth in the January 14, 2004, Office Action on pages 6 and 7, claims 2, 5, 9, 11, 14 and 18 are obvious under 35 U.S.C. § 103(a) based upon:

A. the Lewis patent; in view of

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

- B. the Sibigtroth, et al. patent; and further in view of
- C. United States Patent no. 5,594,319 entitled "Battery Pack Having Theft Deterrent Circuit" that issued January 14, 1997, on a patent filed by Iilonga P. Thandiwe ("the Thandiwe patent").

Claim Groups

As specified below, claims 1-18 do not stand or fall together.

- I. Claims 1-3, 5, 9-12, 14 and 18 stand or fall together.
- II. Claims 4 and 13 stand or fall together.
- III. Claims 7 and 16 stand or fall together.
- IV. Claims 8 and 17 stand or fall together.
- V. Claims 6 and 15 stand or fall together.

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

Argument

Table of Contents

The Cited References	8
The Lewis Patent	8
The Sibigtroth, et al. Patent	9
The Chao Patent	12
The Thandiwe Patent	13
<u>Legal Principles Applicable</u> <u>to Obviousness Rejections</u>	14
Claims 1-3, 5, 9-12, 14 and 18 Are Patentable	18
The Lewis and Sibigtroth, et al. Patents Fail to Produce The Claimed Structure	20
There Exists No Motivation to Combine the Lewis and Sibigtroth, et al. Patents	22
Claims 4 and 13 Are Patentable	25
Claims 7 and 16 Are Patentable	28
Claims 8 and 17 Are Patentable	31
Claims 6 and 15 Are Patentable	35
<u>Objective Evidence of Patentability:</u> <u>Failure of Others</u>	39
The Combined Lewis and Sibigtroth, et al. Patents: A Failed Attempt to Produce a Desired Property	41

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

The Cited References

The Lewis Patent

The Lewis patent discloses an electronic security system that includes a microcomputer which executes a power-on routine stored in a ROM (32) whenever the microcomputer (10) is initially turned-on. Using a keypad 24 connected to microcomputer (10), a user must enter a primary security code (password) which is compared to a predetermined code (user password). If the codes (password and user password) match, the microcomputer (10) signals a main power relay (22) to provide electrical power to the device, thereby enabling the device's operation. Once the device is enabled, the user need not reenter the security code so long as the external source of power to the device remains uninterrupted. (Abstract)

In operation, a device incorporating the present invention is supplied with external power, typically by coupling line 16 to a household A.C. outlet. The logic power supply 12 converts the A.C. current into a D.C. source and provides the requisite D.C. current on line 17. Microcomputer 10, upon the application of power to the power supply 12 executes a power-on routine which is stored in ROM 32. The power-on routine, as will be described, requires the microcomputer to await the input of a code from keypad 24. As the user inputs a code, microcomputer 10 compares the keyed in security code keystroke by keystroke with a predetermined primary security code stored in PROM 34. If the codes match, microcomputer 10 signals the relay driver 18 on line 36 to provide A.C. power to the device by activating the main power relay 22. Power is thereby provided to the device's main power supply 37, or other applicable circuit depending on the nature of the device protected. (Col. 3, lines 41-59.) (Emphasis supplied.)

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

The title of the Lewis patent is "Electronic Security System for Externally Powered Devices". Beginning in column 6 at line 59, the Lewis patent expressly declares the invention's property that:

[a] thief who removes a device protected by the present invention will be unable to use the device, and thus once aware that the device is so protected will likely be deterred from removing it. (Emphasis supplied.)

The Sibigtroth, et al. Patent

The Sibigtroth, et al. patent discloses a "data processor with memory within a single integrated circuit package [that] provides a programmable 'secure mode' of operation to selectively restrict access and protect information stored in its memory." (Abstract)

The data processing system 10 includes a single integrated circuit package portion 11 and a peripheral portion 12 having an external peripheral device. (Col. 2, lines 19-22) The integrated circuit package portion 11² includes:

1. a memory 13;
2. a data processor 14;
3. a decoder 16;

² Attached hereto as Appendix II is a copy of a "Declaration of Brian Oh," which was included in Appellants response to the final rejection of claims in the January 14, 2004, Office Action. Exhibit A included in the "Declaration of Brian Oh," is a copy of FIG. 1 of the Sibigtroth, et al. patent that has been annotated with a dashed line to encloses the integrated circuit package portion 11 of the data processing system 10. (Col. 2, lines 26-49)

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

4. an instruction inhibit circuit 18; and
5. a programmable security device 20. (Col. 2, lines 22-25)

The integrated circuit has memory with programmable security from unauthorized observation of internal processing operations in response to receipt of externally provided signals. (Col. 1, line 49-53)

The integrated circuit package portion 11 operates in three different modes:

1. a "single chip mode;"
2. an "expanded mode;" and
3. a "secure mode." (Abstract)

When the integrated circuit package portion 11 operates in the "single chip mode," the data processor 14 accesses both data and instructions strictly from within the integrated circuit package portion 11. (Abstract) "The single chip mode of operation requires data processor 14 to address predetermined memory locations of memory 13 via address bus 22 for the purpose of either reading instructions and data from memory 13 or writing data to memory 13." (Col. 3, lines 3-8) "The single chip mode is characterized by the fact that only memory 13 and data processor 14, along with address bus 22 and data/instruction bus 24 are utilized." (Col. 3, lines 12-14)

When the integrated circuit package portion 11 operates in the "expanded mode," the data processor 14 may access either the

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

internal memory 13 or external memory for both instructions and data. (Abstract)

In the expanded mode of operation, data processor 14 can access either memory 13 or peripheral portion 12 for both instructions and data. Expanded mode operation utilizes memory 13, data processor 14, address bus 22, data/instruction bus 24, data/instruction bus 30 and instruction inhibit circuit 18. Since expanded mode operation allows data processor 14 to read instructions from peripheral portion 12, the instructions presented to data processor 14 via data/instruction buses 24 or 30, may be readily observed or interrupted for the purpose of reading or modifying the contents of memory 13; therefore the expanded mode of operation is not secure. (Col. 3, lines 19-31) (Emphasis supplied.)

The "secure mode" of operation restricts accesses of instructions to memory contained within the single integrated circuit while allowing data accesses to memory either internal or external to the integrated circuit." (Abstract)

"The secure mode of operation is a mix between the single chip and the expanded modes of operation. In the secure mode of operation, instruction read cycles performed by the data processor are confined to the data processor as in the single chip mode, whereas data reads and writes initiated by the data processor can be made either internal or external to the data processor in an expanded mode of operation. The secure mode of operation provided herein is an effective and economical solution to isolate instruction information of a data processor while allowing the data processor to read or write non-proprietary data external to the data processor.

* * *

However, regardless of the variety of operations considered permissible within a single chip or expanded mode of operation, the functionality of the secure mode insures that memory 13 may not be read or modified by unauthorized sources external to the single integrated circuit package. (Col. 4, lines 34-60) (Emphasis supplied.)

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

The Chao Patent

The Chao patent discloses a computer having an access control device that includes a casing located in a space in the computer that usually receives one of the computer's disk drives. A password may be entered using a keypad that is located on the front panel of the casing. A control unit included in the casing has a memory which stores a password, and a microprocessor unit which receives the input password from the keypad. If the password received from the keypad matches to password stored in the memory unit, the microprocessor generates an activating signal for at least one control circuit connected to the computer keyboard, the floppy disk drive and/or the main system board. The activating signal from the microprocessor unit unlocks and enables the computer keyboard, the floppy disk drive and/or the main system board to permit normal operation of the computer. (Abstract)

The main system board (44) starts booting after the master password has been keyed in (Step 52). A "#" function key on the keypad (2) may be operated anytime during the normal operation of the computer (4) so as to disable the floppy disk drive (41) when it is necessary for the user to leave the computer (4) for a short period of time (Step 53). This obviates the need to turn off the computer (4) in order to prevent unauthorized use of the same, as is required in conventional control devices. Enabling of the floppy disk drive (41) can be accomplished by simply keying in the master password (Step 54). Note that the floppy disk drive (41) is not enabled if an incorrect master password is keyed in.

A "KEYLOCK" function key on the keypad (2) may also be operated anytime during the normal operation of the computer (4) so as to lock the computer keyboard (42) when it is necessary for the user to leave the computer

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

(4) for a short period of time (Step 55). The computer keyboard (42) is unlocked by simply keying in the master password or the secondary password (Step 56). The computer keyboard (42) remains locked if an incorrect master or secondary password is keyed in. (Col. 3, lines 31-52)

The Thandiwe Patent

The Thandiwe patent discloses a battery pack (10) includes a memory (26) for storing a password. Upon connecting the battery pack (10) to a host device (12), the battery waits for a data word to be communicated from the host device over a communications channel (22). If an incorrect data word is received a predetermined number of time, or if an initial power time period, as defined by a timer (30), elapses, a switch (16) is opened, thereby disconnecting the battery cell or cells (14) from the load.
(Abstract)

The operation disclosed in the Thandiwe patent is diametrically opposed to that disclosed in the Lewis, Sibigtroth and Chao patents, and in the present application. The Lewis, Sibigtroth and Chao patents and the present application all disclose a device which remains substantially unenergized until a correct password has been entered. The Thandiwe patent discloses a device which initially is fully energized, and which becomes de-energized if a correct password is not entered within a specified interval.

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

Legal Principles Applicable
to Obviousness Rejections

Certain well established principles must be applied in assessing if an invention is patentable under 35 U.S.C. 103(a). First, the claims of a patent, which define the invention, are "to be construed in light of the specification and both are to be read with a view to ascertaining the invention." United States v. Adams, 383 U.S. 39, 49, 148 USPQ 479, 482 (1966). (Emphasis supplied.) The "differences between the prior art and the claims at issue are to be ascertained." Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966). (Emphasis supplied.) Moreover, it is elementary that the claimed invention must be considered as a whole in deciding obviousness. Litton Industrial Products, Inc. v. Solid State Systems Corp., 755 F.2d 158, 164, 225 USPQ 34, 38 (Fed. Cir. 1985). (Emphasis supplied.) The prior art as a whole must be considered, and those portions of the prior art arguing against or teaching away from the claimed invention must be considered. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc., 796 F.2d 443, 448, 230 USPQ 416, 420 (Fed. Cir. 1986), In re Hedges, et al., 783 F.2d 1038, 1041, 228 USPQ 685, 687 (Fed. Cir. 1986). (Emphasis supplied.)

An invention is obvious under 35 U.S.C. § 103(a), only if the prior art suggests a modification of the reference(s) and/or their combination. In In re Gordon, 733 F.2d 900, 902, 221 USPQ 1125,

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

1127 (Fed. Cir. 1984) the Court of Appeals for the Federal Circuit reversed a Board of Appeals decision that a patent application's claims were obvious under 35 U.S.C. § 103 holding "that although a prior art [fuel filter] device could have been turned upside down, that did not make the modification obvious unless the prior art fairly suggested the desirability of turning the device upside down." Continental Can Co. USA, Inc. v. Monsanto Co. 948 F.2d 1264, ___, 20 USPQ2d 1746, 1751 (Fed. Cir. 1991). "The mere fact that the prior art could be . . . modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." In re Gordon, supra at 221, 1127. In accord, In re Laskowski, 871 F.2d 115, 117, 10 USPQ2d 1397, 1398 (Fed. Cir. 1989). "[E]lements of separate prior patents cannot be combined when there is no suggestion of such combination anywhere in those patents". Panduit Corp. v. Dennison Manufacturing Co., 810 F.2d 1561, 1568, 1 USPQ2d 1593, 1597 (Fed. Cir. 1987) citing ACS Hospital Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). (Emphasis supplied.) An examiner is obliged to explain why combining references is proper indicating why one skilled in the art would make a combination or substitution. Ex parte Skinner, 2 USPQ2d 1788, 1790 (Bd. Pat. App. & Int. 1986).

The motivation, suggestion or teaching may come explicitly from statements in the prior art, the knowledge of one of ordinary skill in the art, or, in some

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

cases the nature of the problem to be solved. See Dembiczak, 175 F.3d at 999, 50 USPQ2d at 1617. In addition, the teaching, motivation or suggestion may be implicit from the prior art as a whole, rather than expressly stated in the references. See WMS Gaming, Inc. v. International Game Tech., 184 F.3d 1339, 1355, 51 USPQ2d 1385, 1397 (Fed. Cir. 1999). The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art. See In re Keller, 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981) (and cases cited therein). Whether the Board relies on an express or an implicit showing, it must provide particular findings related thereto. See Dembiczak, 175 F.3d at 999, 50 USPQ2d at 1617. Broad conclusory statements standing alone are not "evidence." Id. In Re Werner Kotzab, 217 F.3d 1365, 1369, 55 USPQ2d 1313, 1316 (Fed. Cir. 2000). (Emphasis supplied.)

In Ecolochem, Inc. v. Southern California Edison Company, 227 F.3d 1361, 1371-72, 56 USPQ2d 1065, 1072-73 (Fed. Cir. 2000), the Court of Appeals for the Federal Circuit declared that:

[i]n In re Dembiczak, we noted that:

Measuring a claimed invention against the standard established by section 103 requires the oft-difficult but critical step of casting the mind back to the time of invention, to consider the thinking of one of ordinary skill in the art, guided only by the prior art references and the then-accepted wisdom in the field.

In re Dembiczak, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999). We "cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." In re Fine, 837 F.2d 1071, 1075, 5 USPQ2d 1780, 1783 (Fed. Cir. 1988).

Our case law makes clear that the best defense against hindsight-based obviousness analysis is the rigorous application of the requirement for a showing of a teaching or motivation to combine the prior art references. See Dembiczak, 175 F.3d at 999, 50 USPQ2d at

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

1617. "Combining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art to defeat patentability--the essence of hindsight." Id.

"When a rejection depends on a combination of prior art references, there must be some teaching, suggestion, or motivation to combine the references." In re Rouffet, 149 F.3d 1350, 1355, 47 USPQ2d 1453, 1456 (Fed. Cir. 1998) (citing In re Geiger, 815 F.2d 686, 688, 2 USPQ2d 1276, 1278 (Fed. Cir. 1987)).

* * *

"Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hosp. Sys., Inc. v. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). Although the suggestion to combine references may flow from the nature of the problem, see Pro-Mold & Tool Co. v. Great Lakes Plastics, Inc., 75 F.3d 1568, 1573, 37 USPQ2d 1626, 1630 (Fed. Cir. 1996), "[d]efining the problem in terms of its solution reveals improper hindsight in the selection of the prior art relevant to obviousness," Monarch Knitting Mach. Corp. v. Sulzer Morat GmbH, 139 F.3d 877, 880, 45 USPQ2d 1977, 1981 (Fed. Cir. 1998). Therefore, "[w]hen determining the patentability of a claimed invention which combines two known elements, 'the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.'" In re Beattie, 974 F.2d 1309, 1311-12, 24 USPQ2d 1040, 1042 (Fed. Cir. 1992) (quoting Lindemann, 730 F.2d at 1462, 221 USPQ at 488). (Emphasis supplied.)

Applying the preceding principles to the claims of the present application and to the various references discussed herein, Appellants respectfully submit that a proper reading both of the claims in light of the specification and of the references, either alone or in combination, fails to disclose or to even suggest the invention embodied in the presently pending claims.

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

Claims 1-3, 5, 9-12, 14 and 18 Are Patentable

In rejecting dependent claims 1 and 10, the January 14, 2004, Office Action alleges:

[a]s per claims 1, and 10, Lewis discloses a device to be used in conjunction with an electronic device, (Col 3 line 4). Lewis discloses that the controller is connected to electrical power even though the controller is not powering the electronic device, (Col 3 line 25). Lewis discloses that the electronic device is energized when a user inputs the correct password, (Col 3 lines 52-56). Lewis teaches that the security controller comprises a nonvolatile password memory, (PROM), for storing at least one user password, (Col 3 lines 50-53). Lewis teaches a password input circuit, a digital logic circuit, and an output circuit (Microcomputer), (Col 3 lines 50-53). The digital logic circuit compares a received password with any user passwords stored in memory, (Col 3 line 50). Lewis shows the output circuit for transmitting a signal to enable the electronic device with power if the received password matches the stored password, (Col 3 lines 52-56).

Lewis does not disclose that an integrated circuit comprises the pre-boot security controller.

Sibitroth discloses a controller and memory as part of an integrated circuit (Sibitroth Col 2 lines 19-25). It would be obvious to one skilled in the art to construct the microcomputer of Lewis in the method of Sibitroth because it is more compact.

In rejecting dependent claims 3 and 12, the January 14, 2004, Office Action alleges based upon the same combination of references as applied in rejecting claims 1 and 10:

[a]s per claims 3, and 12, there is at least one user password, and at least one supervisor password, (secondary password), (Col 4 lines 34-37).

In rejecting dependent claims 2 and 11, the January 14, 2004, Office Action alleges based upon the same combination of references as applied in rejecting claims 1 and 10:

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

[a]s per claims 2, and 11, Lewis does not disclose that the password memory is electronically rewritable, (Col 3 lines 8-11).

Thandiwe discloses the password memory to be EEPROM, which is rewritable memory.

In rejecting dependent claims 5 and 14, the January 14, 2004, Office Action alleges based upon the same combination of references as applied in rejecting claims 1 and 10:

[a]s per claims 5, and 14, Lewis discloses a keypad interface, and that the interface may receive passwords. Lewis fails to disclose the digital logic recording such passwords. Thandiwe discloses choosing a new password and storing it in the password memory, (Col 3 line 16).

It would be obvious to one skilled in the art, to modify Lewis's security controller with Thandiwe's password storage so that a password may be changed on a regular basis to enhance security.

In rejecting dependent claims 9 and 18, the January 14, 2004, Office Action alleges based upon the same combination of references as applied in rejecting claims 1 and 10:

[a]s per claims 9 and 18, Lewis does not disclose a "System Management Bus" to receive user passwords to store in memory.

Thandiwe discloses receiving a password over a system management bus, (Col 2 lines 20-25).

It would be obvious to one skilled in the art, to modify Lewis's security controller with Thandiwe's system management (sic) because an internal SMBus connection is more secure than a line or cable connection.

The rejections of claims 1-3, 5, 9-12, 14 and 18 excerpted above from the January 14, 2004, Office Action all depend either exclusively upon a combination of the Lewis and Sibigtroth, et al. patents, or upon those two (2) references combined with yet another reference. Thus, if claims 1 and 10 are patentable over the

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

combined Lewis and Sibigtroth, et al. patents, then claims 2, 3, 5, 9, 11-12, 14 and 18 respectively depending therefrom are also patentable.

The Lewis and Sibigtroth, et al. Patents Fail to Produce The Claimed Structure

Independent claims 1 and 10 encompass:

If the microcomputer 10 of the Lewis patent were merely constructed in the method of the Sibigtroth, et al. patent as presented in the January 14, 2004, Office Action, storage for the predetermined primary security code, i.e. predetermined primary password, still remains in the PROM 34 outside the integrated circuit microcomputer 10. Moreover, if the microcomputer 10 of the Lewis patent were constructed in the method of the Sibigtroth, et al. patent retaining the PROM 34 outside the integrated circuit microcomputer 10 for storing the predetermined primary security code, i.e. predetermined primary password, then:

1. the combined references produces a structure that is no more compact than the disclosure of the Lewis patent alone; and

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

2. the motivation alleged in the January 14, 2004, Office Action for combining the two references fails to exist.

Therefore, Appellants respectfully submit that independent claims 1 and 10 traverse rejection for obviousness under 35 U.S.C. § 103(a) based the Lewis and Sibigtroth, et al. patents as combined in the January 14, 2004, Office Action because:

1. that combination leaves password storage outside the integrated circuit microprocessor 10; and
2. the motivation alleged for combining the references does not exist.

Furthermore, if the microcomputer 10 of the Lewis patent were constructed in the method of the Sibigtroth, et al. patent, and if the PROM 34 were omitted and if the predetermined primary security code, i.e. predetermined primary password, were stored in the memory 13 of the Sibigtroth, et al. patent's integrated circuit package portion 11, then the combination lacks non-volatile password storage. Consequently, if one were to construct the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent and were to store the predetermined primary security code, i.e. predetermined primary password, in the memory 13 of the integrated circuit package portion 11, due to a lack of non-volatile storage the predetermined primary security code, i.e. predetermined primary password, would be forever lost if electrical power were removed from the integrated circuit package

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

portion 11. Since the preceding hypothetical combination of the disclosures of the Lewis and Sibigtroth, et al. patents that appears nowhere in the January 14, 2004, Office Action results in loss of the predetermined primary security code, i.e. predetermined primary password, upon removal of electrical power, independent claims 1 and 10 traverse rejection for obviousness under 35 U.S.C. § 103(a) based upon the hypothetical combination because:

1. the combination is inoperable for the Lewis patent's intended purpose; and
2. their exists no motivation for combining references which produces a device that is inoperable for its intended purposes.

There Exists No Motivation to Combine the Lewis and Sibigtroth, et al. Patents

In rejecting independent claims 1 and 10, the January 14, 2004, Office Action first acknowledges:

Lewis does not disclose that an integrated circuit comprises the pre-boot security controller.

The January 14, 2004, Office Action then alleges that:

Sibitroth discloses a controller and memory as part of an integrated circuit (Sibitroth Col 2 lines 19-25). It would be obvious to one skilled in the art to construct the microcomputer of Lewis in the method of Sibitroth because it is more compact.

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

Appellants respectfully submit that one searches the Lewis and the Sibigtroth, et al. patents vainly for any mention that size is a problem, or that the invention disclosed in the Sibigtroth, et al. patent makes things smaller. The title of the Lewis patent is "Electronic Security System for Externally Powered Devices". Beginning in column 6 at line 59, the Lewis patent expressly declares that its invention provides theft deterrence.

A thief who removes a device protected by the present invention will be unable to use the device, and thus once aware that the device is so protected will likely be deterred from removing it. (Emphasis supplied.)

The title of the Sibigtroth, et al. patent is "Integrated Circuit Microcontroller with On-Chip Memory and External Bus Interface and Programmable Mechanism for Securing the Contents of On-Chip Memory." The Sibigtroth, et al. patent identifies the following problems which its invention allegedly solves.

1. There is often a need to prevent read or write accesses to . . . memory elements for various security reasons. (Col. 1, lines 19-21.)
2. [M]emory space within the chip is typically limited, the instructions and data contained within the chip are also limited in size. (Col. 1, lines 32-34.)
3. Another disadvantage with a security feature requiring a single-chip mode of operation is the inability to communicate with any peripheral devices external to the chip. (Col. 1, lines 38-41.)

Because neither the Lewis patent nor the Sibigtroth, et al. patents disclose nor do they suggest that there exists any size problem, Appellants respectfully submit that the motivation alleged

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

in the January 14, 2004, Office Action, i.e. that "[i]t would be obvious to one skilled in the art to construct the microcomputer of Lewis in the method of Sibitroth because it is more compact," comes not from the cited references, nor does it come from any general desire to provide enhanced theft deterrence for electronic devices. Rather, Appellants respectfully submit that the motivation to combine the Lewis and Sibigtroth, et al. patents comes from a need to reject claims pending in the present patent application.

Because for the reasons set forth above the alleged motivation for combining presented in the January 14, 2004, Office Action is a canard, Appellants respectfully:

1. submit that independent claims 1 and 10, together with all claims depending therefrom including dependent claims 2, 3, 5, 9, 11-12, 14 and 18, traverse rejection under 35 U.S.C. § 103(a) for obviousness because there truly exists no motivation for combining the Lewis and Sibigtroth, et al. patents other than the present patent application; and
2. request that independent claims 1 and 10, together with all claims depending therefrom including dependent claims 2, 3, 5, 9, 11-12, 14 and 18, be declared patentable.

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

Claims 4 and 13 Are Patentable

In rejecting dependent claims 4 and 13, the January 14, 2004, Office Action, using the disclosures of the combined Lewis and Sibigtroth, et al. patents as applied above to independent claims 1 and 10, alleges:

[a]s per claims 4, and 13, the input circuit is a keypad interface (Mc) that is coupled to a keypad for receiving a password to be compared with stored passwords, (Col 3 line 48).

The texts of pending claims 4 and 13 recite specific characteristics which the "password input circuit," respectively of independent claims 1 and 9, must possess. Thus, pending claim 4 recites that:

said password input circuit is a keypad interface that is adapted to be coupled to a security keypad for receiving the password that a user of the electronic device enters using the security keypad for comparison with user passwords recorded in said password memory. (Emphasis supplied.)

In a similar manner, the text of pending claim 13 recites that:

said password input circuit included in said pre-boot security controller is a keypad interface, the electronic device further comprising a security keypad that is coupled to the keypad interface to transmit thereto for comparison with user passwords recorded in said password memory the password that a user of the electronic device enters using the security keypad.

An antecedent for the phrase "security keypad" appearing in the text of the patent application's specification establishes that the term has a particular meaning in the context of dependent claims 4 and 13. The pending application on page 10 beginning in

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

line 8 describes a preferred embodiment for the password input circuit as follows:

The pre-boot security controller 42 also includes a password input circuit 82 which is a keypad input circuit in the preferred embodiment illustrated in FIG. 2. As better illustrated in FIG. 1, a keypad bus 84 couples the password input circuit 82 to a 4-button security keypad 86.

* * *

One class of security keypad 86 employs scanning similar to that used for a conventional personal computer keyboard. This class of keypad supplies a patterned scanning output to the keys while monitoring every key's input. A match between the patterned scanning output and a key indicates that the key is being pressed. The other class of security keypad 86 provides individual switches for each of the keys. Each switch included in the keypad has its own output terminal. For switch type keypads pressing a key grounds the signal at that key's output terminal.

The sentence which the January 14, 2004, Office Action identifies in the Lewis patent for finally rejecting dependent claims 4 and 13 appears in the following excerpt.

The power-on routine, as will be described, requires the microcomputer [10] to await the input of a code from keypad 24. (Col. 3, lines 48-50.)

As is readily apparent from the preceding sentence, the text of the Lewis patent in column 3 at line 48 fails to disclose anything other than the microcomputer 10, denoted Mc 10 in FIG. 1, and also fails to disclose anything resembling the security keypad 86 described in the pending patent application's text. Because the Lewis patent in column 3 at line 48 fails to expressly disclose the keypad interface adapted to be coupled to a security keypad as

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

encompassed by dependent claims 4 and 13, in rejecting these claims
the January 14, 2004, Office Action must necessarily rely upon
inherency.

"The mere fact that a certain thing may result from a given set of circumstances is not sufficient" for inherency. Ex parte Skinner, 2 USPQ2d 1788, 1789 (Bd. Pat. App. & Int. 1986). If a claimed invention is not clearly anticipated by a reference, i.e. if the invention is not fully disclosed in a single prior art reference or embodied in a single practice or device, arguments of inherency are immaterial. Jones et al. v. Hardy, 727 F.2d 1529-30, 220 USPQ 1021, 1025-26 (Fed. Cir. 1984). (Emphasis supplied.) Inherency . . . may not be established by probabilities or possibilities. "'That which may be inherent is not necessarily known. Obviousness cannot be predicated on what is unknown." In re Newell, 891 F.2d 899, 901, 13 USPQ2d 1248, 1250 (Fed. Cir. 1989). (Emphasis supplied.)

The Lewis patent in column 3 at line 48 fails to expressly disclose the keypad interface as encompassed by pending claims 4 and 13. Consequently, the combined Lewis and Sibigtroth, et al. patents neither disclose nor do they suggest the "keypad interface" as that phrase is used in claims 4 and 13 and throughout the pending application. Therefore, Appellants respectfully:

1. submit that the controlling legal authority cited above mandates that dependent claims 4 and 13 traverse the

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

rejection under 35 U.S.C. § 103(a) for obviousness which appears in the January 14, 2004, Office Action; and

2. request that dependent claims 4 and 13 be declared patentable.

Claims 7 and 16 Are Patentable

In rejecting dependent claims 7 and 16, the January 14, 2004, Office Action, using the disclosures of the combined Lewis and Sibigtroth, et al. patents as applied above to independent claims 1 and 10, alleges:

[a]s per claims 7, and 16, the digital logic circuit is a state machine (Microcomputer), (Col 3 line 60).

Applicant's respectfully submit that the phrase "state machine" as used in the present application has a particular meaning which differs from that of the word microcomputer as used in the Lewis patent. While the phrase "state machine 52" appears frequently in the pending patent application's text, Appellants respectfully submit that the following two excerpts from the pending application sufficiently establish the phrase's meaning.

Referring now to FIG. 2, the pre-boot security controller 42 includes a clock control 48 that supplies a CLK signal to a digital logic state machine 52. Operation of the state machine 52 may place the pre-boot security controller 42 into any one of three different operating modes. (P. 9, lines 5-10.)

Transition of the state machine 52 from the security operating mode to the application operating mode causes the output control 62 to negate the signals present on

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

the OUT_PWR# signal-line 64 and the OUT_SUS# signal-line 66 which causes the DC/DC converter 32 to energize the operation of the remainder of the electronic device 20. (P. 12, lines 6-11.)

The National Institutes of Standards and Technology's ("NIST's") "Dictionary of Algorithms and Data Structures" ("DADS") defines the phrase "state machine" as follows.

An abstract computer consisting of a (possibly infinite) set of states, a set of start states, an input alphabet, and a transition function which maps input symbols and current states to a next state. Usually understood to be a finite state machine.

DADS also defines the phrase "finite state machine" as:

[a] model of computation consisting of a set of states, a start state, an input alphabet, and a transition function that maps input symbols and current states to a next state. Computation begins in the start state with an input string. It changes to new states depending on the transition function. There are many variants, for instance, machines having actions (outputs) associated with transitions (Mealy machine) or states (Moore machine), multiple start states, transitions conditioned on no input symbol (a null) or more than one transition for a given symbol and state (nondeterministic finite state machine), one or more states designated as accepting states (recognizer), etc.

Also known as finite state automaton.

Now compare the characteristics of the phrase "state machine" as described in the pending application and in the NIST's DADS definitions with the "microcomputer 10" as described in the Lewis patent.

Referring now to FIG. 1, the present invention includes as a part thereof a microcomputer indicated by Numeral 10. The microcomputer can be any one of a variety of types currently commercially available. It

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

will be appreciated from the discussion which follows that an existing on-board microcomputer of the type typically used in frequency-synthesized tuning systems in television and radio may be utilized, with little modification to those devices which incorporate such tuning systems.

* * *

The microcomputer 10 is coupled to a keypad 24 by line 25, and to a digital display 26 by line 28. In addition, microcomputer 10 is coupled to a read-only memory (ROM) 32 and to a programmable read-only memory (PROM) 34. As will be discussed more fully below, the ROM 32 contains a power-on sequence of operations which the microcomputer performs whenever external A.C. power is initially supplied on line 16. (Col. 3, lines 15-40.)

It is readily apparent from the preceding description that the Lewis patent uses the word "microcomputer" to describe a device which is more commonly known today as a "microprocessor." The "microcomputer 10" of the Lewis patent, i.e. "microprocessor," is coupled to a "read-only memory (ROM) 32" from which it fetches and executes "a power-on sequence of operations . . . whenever external A.C. power is initially supplied on line 16."

Now further compare the preceding description for the Lewis patent's "microcomputer" and the illustration thereof in FIG. 1 of the Lewis patent, attached hereto as Appendix III, with the "state machine" that appears in FIG. 2 of the pending application, attached hereto as Appendix IV. While the state machine 52 depicted in FIG. 2 connects to a flash memory 56 which is equivalent to the PROM 34 depicted in FIG. 1 of the Lewis patent, the state machine 52 depicted in FIG. 2 of the pending application lacks:

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

the ROM 32 [which] contains a power-on sequence of operations which the microcomputer performs whenever external A.C. power is initially supplied on line 16. (The Lewis patent in col. 3 at lines 37-40.)

The preceding facts establish that the phrase "state machine" as used in dependent claims 7 and 16 differs patentably from the "microcomputer 10," i.e. "microprocessor," disclosed in the Lewis patent. Furthermore, the combined Lewis and Sibigtroth, et al. patents neither disclose nor do they suggest a "state machine" as that phrase is used in claims 7 and 16 and throughout the pending application. Therefore, Appellants respectfully:

1. submit that the "state machine" encompassed by dependent claims 7 and 16 traverses the rejection for obviousness under 35 U.S.C. § 103(a) that appears in the January 14, 2004, Office Action based upon the combined Lewis and Sibigtroth, et al. patents; and
2. request that dependent claims 7 and 16 be declared patentable.

Claims 8 and 17 Are Patentable

In rejecting dependent claims 8 and 17, the January 14, 2004, Office Action, using the disclosures of the combined Lewis and Sibigtroth, et al. patents as applied above to independent claims 1 and 10, alleges:

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

[a]s per claims 8, and 17, the output circuit provides a signal, which indicates the existence of the security operating mode (alarm), (Col 4 line 61, Col 5 line 1).

The text cited in the preceding rejection of claims 8 and 17 appears in the following excerpt from the Lewis patent.

As shown in FIG. 2, if the first digit or character entered by the user does not match either the primary security code or the secondary code as discussed above, the microcomputer enters an alarm mode and displays "HOT" or some other similar message in the digital display 26 and does not enable the main power relay 22 through the relay driver 18. Thus, until power is removed, by for example removing the A.C. plug, the microcomputer will not permit further keyboard entries and will not enable power to be coupled to the protected device through the main power relay 22. As illustrated in FIG. 2, the alarm mode may include an optional audible alarm tone in the form of a warble generated by the microcomputer as a digital pulse train of varying period, and incorporate a flashing digital display. As depicted, if the first inputted digit matches with either the stored primary or secondary code, any subsequent digit which when compared fails to match will automatically send the microcomputer into the alarm mode. (Col. 4, line 57 - col. 5, line 8.) (Emphasis supplied.)

The preceding text establishes that the Lewis patent's "alarm mode" acts to immediately indicate entry of an incorrect password character.³

³ Applicants respectfully submit that the "alarm mode" disclosed in the Lewis patent significantly compromises any security that the patent's invention might provide. As illustrated in FIG. 1, the keypad 24 includes 18 keys. The Lewis patent's "alarm mode" operates to immediately indicates entry of an incorrect password character. Thus, by sequentially pressing keys on the keypad 24, on average it will take only nine (9) trials to determine a password's first character. Knowing the password's first character, the flowchart in FIG. 2 of the Lewis patent indicates that on average it will then

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

Now compare the "alarm mode" disclosed in the Lewis patent with the "security operating mode" of pending dependent claims 8 and 17. Dependent claims 8 and 17 encompass providing "an output signal which indicates the existence of the security operating mode." The text of the pending application beginning on page 9 in line 11 describes the "security operating mode" as follows.

When the DC/DC converter 32 first supplies VCC electrical power to the pre-boot security controller 42, a signal supplied to the pre-boot security controller 42 via a RST# signal-line 54 is negated and a password has been previously recorded into a 512 byte nonvolatile, electronically rewritable flash memory 56, the pre-boot security controller 42 enters a security operating mode. When the pre-boot security controller 42 is in the security operating mode, an output control 62, included in the pre-boot security controller 42, transmits signals to the DC/DC converter 32 via a OUT_PWR# signal-line 64

take only nine (9) trials to determine the password's second character. If a password contains only three (3) characters as illustrated in FIG. 2, then on average the entire password can be determined after only twenty-seven (27) trials. The Lewis patent's three (3) character password can always be determined after only fifty-four (54) trials because the "alarm mode" immediately indicates when the "digit or character entered by the user does not match either the primary security code or the secondary code." Increasing the number of characters in a password to five (5), i.e. the number of characters described in the present application on page 14 in lines 19-24, only increases the maximum number of trials required determine the password to ninety (90) due to the Lewis patent's alarm mode. The preceding analysis of the Lewis patent demonstrates that its passwords can be easily cracked, if not manually, then certainly by a simple automatic apparatus which recursively exercises the device one keystroke at a time to record and reuse those keystrokes which the apparatus determines do not produce the alarm mode signal.

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

and an OUT_SUS# signal-line 66 that inhibit the DC/DC converter 32 from energizing operation of the digital computer 22, and other portions of the electronic device 20 not illustrated in FIG. 1. Thus, while the signals present on the OUT_PWR# signal-line 64 and OUT_SUS# signal-line 66 are asserted, the electronic device 20, except for the pre-boot security controller 42, the clock control 48 and a portion of the DC/DC converter 32, is inoperable. Moreover, to apprise a user of the electronic device 20 that the pre-boot security controller 42 is in the security operating mode, the output control 62 transmits a signal on a LED signal-line 68 which illuminates a LED included in a status output subsystem 72 illustrated in FIG. 1. (Emphasis supplied.)

When the user enters a password that is recorded in the flash memory 56, the state machine 52 exits the security operating mode and enters an application operating mode thereby operationally unlocking the electronic device 20. Transition of the state machine 52 from the security operating mode to the application operating mode causes the output control 62 to negate the signals present on the OUT_PWR# signal-line 64 and the OUT_SUS# signal-line 66 which causes the DC/DC converter 32 to energize the operation of the remainder of the electronic device 20. (Page lines 2-11.)

The text excerpted above from the present application clearly establishes that the "security operating mode" exists immediately after electrical power is first supplied to the pre-boot security controller 42 and continues throughout the interval in which the state machine 52 operates for password entry.

The preceding facts establish that the "output signal which indicates the existence of the security operating mode" of dependent claims 8 and 17 differs patentably from the "alarm mode"

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

signal disclosed in the Lewis patent.⁴ Furthermore, the combined Lewis and Sibigtroth, et al. patents neither disclose nor do they suggest providing "an output signal which indicates existence of the security operating mode" as recited in dependent claims 8 and 17, and as the phrase "security operating mode" is used in the present application. Therefore, Appellants respectfully:

1. submit that the "output signal which indicates the existence of the security operating mode" encompassed by dependent claims 8 and 17 traverses the rejection for obviousness under 35 U.S.C. § 103(a) that appears in the January 14, 2004, Office Action based upon the combined Lewis and Sibigtroth, et al. patents; and
2. request that dependent claims 8 and 17 be declared patentable.

Claims 6 and 15 Are Patentable

In rejecting dependent claims 6 and 15, the January 14, 2004, Office Action, based upon the same combination of references as applied in rejecting claims 1 and 10 together with the Chao patent, alleges:

⁴ Note that the present application's "security operating mode" does not compromise password security by immediately indicating the entry of an incorrect password character in comparison with the Lewis patent's "alarm mode" which compromises security by immediately indicating incorrect password character entry.

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

[a]s per claims 6, and 15, Lewis discloses a security controller that receives a user password and matches it to that in memory, (Col 3 line 50).

Lewis does not disclose taking input from the keypad in application operating mode.

Chao discloses a keypad that prevents booting of the computer and is of an analogous art to the instant specification. To utilize the keypad pressings, the data must be recorded, (Col 3 line 33, 44).

It would be obvious to one skilled in the art to modify Lewis's security controller with Chao's application mode keypad operation because it obviates the need to turn off the computer (Col 3 line 37).

The following text from the Chao patent which begins in column 3 at line 41 includes the text identified above in the January 14, 2004, Office Action.

A "#" function key on the keypad (2) may be operated anytime during the normal operation of the computer (4) so as to disable the floppy disk drive (41) when it is necessary for the user to leave the computer (4) for a short period of time (Step 53). This obviates the need to turn off the computer (4) in order to prevent unauthorized use of the same, as is required in conventional control devices. Enabling of the floppy disk drive (41) can be accomplished by simply keying in the master password (Step 54). Note that the floppy disk drive (41) is not enabled if an incorrect master password is keyed in.

A "KEYLOCK" function key on the keypad (2) may also be operated anytime during the normal operation of the computer (4) so as to lock the computer keyboard (42) when it is necessary for the user to leave the computer (4) for a short period of time (Step 55). (Emphasis supplied.)

The preceding excerpt from the Chao patent clearly describes pressing a particular key, i.e. the "'#' function key on the keypad (2)," "to disable the floppy disk drive (41)" followed by "simply

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

keying in the master password" to enable "the floppy disk drive (41)."

Dependent claims 6 and 15 encompass "an application operating mode in which the pre-boot security controller preserves data about pressings of the security keypad." The text of the pending application beginning on page 25 at line 11 describes this particular operation of the pre-boot security controller.

When the pre-boot security controller 42 is in the application operating mode it responds to pressing any key 102 through 112 of the security keypad 86 by storing in the register block 142 data indicating which key 102 through 112 has been pressed, and by transmitting a SMBus alert, i.e. an interrupt, to the SMBus host 126. The computer program executed by the digital computer 22, after interrogating the pre-boot security controller 42 via the SMBus 124 to determine which key 102 through 112 has been pressed, may respond appropriately to that event. Specifically, it is envisioned that the computer program may be advantageously enabled to respond to pressing any of the keys 102 through 112 by initiating execution of a specific application computer program that has been associated with a specific key 102 through 112 by a user of the electronic device 20 prior to the key pressing event.

The register included in the register block 142 which stores the data that indicates which of the keys 102 through 112 has been pressed stores such data for only one of the keys 102 through 112. Subsequent pressings of any of the keys 102 through 112 after one key 102 through 112 has been pressed are ignored until the computer program executed by the digital computer 22, accessing the register block 142 via the SMBus 124, clears the register in the register block 142 which stores the key pressing data. (Emphasis supplied.)

Clearly the pre-boot security controller's preservation of "data about pressings of the security keypad" described in the present application differs entirely from the Chao patent's

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

disclosure that pressing the "'#' function key on the keypad (2)" disables "the floppy disk drive (41)." Rather than disabling anything, the pre-boot security controller preserves data about which of the keys 102 through 112 has been pressed to become input data used by a computer program while the pre-boot security controller remains in its application operating mode. In the context of the present patent application, effecting an operation analogous to that of the Chao patent requires a transition from pre-boot security controller's application operating mode to its security operating mode, i.e. an operation not encompassed by the text of dependent claims 6 and 15.

The preceding facts establish that "an application operating mode in which the pre-boot security controller preserves data about pressings of the security keypad" encompassed by dependent claims 6 and 15 differs patentably from the Chao patent's disclosure that pressing the "'#' function key on the keypad (2)" disables "the floppy disk drive (41)." Furthermore, the combined Lewis, Sibig-troth, et al. and Chao patents neither disclose nor do they suggest providing an operating mode in which data about pressings of a keypad are preserved as encompassed by dependent claims 6 and 15, and as described in the present application. Therefore, Appellants respectfully:

1. submit that the "an application operating mode in which the pre-boot security controller preserves data about

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

pressings of the security keypad" encompassed by dependent claims 6 and 15 traverses the rejection for obviousness under 35 U.S.C. § 103(a) that appears in the January 14, 2004, Office Action based upon the combined Lewis, Sibigtroth, et al. and Chao patents; and

2. request that dependent claims 6 and 15 be declared patentable.

**Objective Evidence of Patentability:
Failure of Others**

A sequence of controlling judicial decisions holds that prior art references which do not enable an invention, specifically references where the disclosure fails for its intended purpose, permit patenting a later invention. The Supreme Court in United States v. Adams supra, affirming patentability over a combination of references, dismissed reliance on a prior 1880 British patent to Skrivanoff. An expert attempted to make the product in accordance with Skrivanoff's teachings "but was met first with a fire . . . and then with an explosion." Adams, at ___, 482. "That in 1880 Skrivanoff may have been able to convince a foreign patent examiner to issue a patent on his device has little significance in the light of the foregoing." Adams, at 50, 483. "To be prior art under section 102(b) the reference must put the anticipating subject matter at issue into the possession of the public through

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

an enabling disclosure." Chester v. Miller, 906 F.2d 1574, 1577 n.2, 15 USPQ2d 1333, 1336 n.2 (Fed. Cir. 1990).

"If obviousness is involved, the invalidity rests on § 103 based on § 102(b) prior art." J.A. LaPorte, Inc. v. Norfolk Dredging Co., 787 F.2d 1577, 1580 n.4, 229 USPQ 435, 437 n.4 (Fed. Cir. 1986), cert. denied, 479 U.S. 884 (1986). "'In order to render a claimed apparatus or method obvious, the prior art must enable one skilled in the art to make and use the apparatus or method.'" Motorola, Inc. v. Interdigital Technology Corp., 121 F.3d 1461, 1471, 43 USPQ2d 1481, 1489 (Fed. Cir. 1997) quoting Beckman Instruments, Inc. v. LKB Produkter AB, 892 F.2d 1547, 13 USPQ2d 1301 (Fed. Cir. 1989). "That prior art patents may have described failed attempts . . . or attempts that used different elements . . . is not enough. The prior art must be enabling." Rockwell International Corp. v. United States, 147 F.3d 1358, 1365, 47 USPQ2d 1027, 1032 (Fed. Cir. 1998) citing Motorola *supra*.

In In re Gurley, 7 F.3d 551, 31 USPQ2d 1130 (Fed. Cir. 1994) decided after Beckman *supra*, the court noted:

A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. The degree of teaching away will of course depend on the particular facts; in general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant. See United States v. Adams, 383 U.S. 39, 52, 148 USPQ 479, 484 (1966) ("known

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

disadvantages in old devices which would naturally discourage the search for new inventions may be taken into account in determining obviousness")

* * *

In re Sponnoble, 405 F.2d 578, 587, 160 USPQ 237, 244 (CCPA 1969) (references taken in combination teach away since they would produce a "seemingly inoperative device"); In re Caldwell, 319 F.2d 254, 256, 138 USPQ 243, 245 (CCPA 1963) (reference teaches away if it leaves the impression that the product would not have the property sought by the applicant). Gurley, at 553, 1131-32.

The Combined Lewis and Sibigtroth,
et al. Patents: A Failed Attempt
to Produce a Desired Property

The property desired for the invention disclosed in the Lewis patent is theft deterrence. Beginning column 6 at line 59, the Lewis patent in expressly declares that:

[a] thief who removes a device protected by the present invention will be unable to use the device, and thus once aware that the device is so protected will likely be deterred from removing it. (Emphasis supplied.)

Appellants first observe that, for reasons explained in greater detail in footnote 3, the Lewis patent's "alarm mode" greatly simplifies a thief's determination of passwords that are stored in the PROM 34. Using information provided by the Lewis patent's "alarm mode" and a brute force password attack,⁵ passwords stored in the PROM 34, on average, can be determined by a repetitive number of trials which equals:

⁵ A "brute force password attack" is one which tries all possible passwords successively one after another until encountering one which works.

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

1. one-half ($\frac{1}{2}$) of the total number of characters enterable using the keypad 24; multiplied by
2. the number of characters in the password.

Due to the Lewis patent's "alarm mode," using brute force passwords stored in the PROM 34 can always be determined by a repetitive number of trials which does not exceed:

1. the total number of characters enterable using the keypad 24; multiplied by
2. the number of characters in the password.

That is, the difficulty of determining passwords stored in the Lewis patent's PROM 34 using a brute force attack only increases linearly with the number of characters in the password due to the reference's "alarm mode."

Conversely, for a security device such as that disclosed in the present application which lacks the Lewis patent's alarm mode, the average number of trials required for a brute force attack on passwords stored in the flash memory 56 equals the number of characters expressible using the keypad 86 raised to the power of the number of characters in the password. That is, if " n " represents the number of characters which may be entered using the keypad 86 and k represents the number of characters in the password, using a brute force password attack the present invention, lacking the Lewis patent's alarm mode, requires, on average, $\frac{1}{2}(n)^k$ trials to determine a password.

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

If as described on page 14 beginning at line 19 of the present application each pressing of the keypad 86 selects one of fifteen (15) characters, and if a password contains the maximum number of five (5) characters, a brute force password attack, on average, requires three-hundred seventy-nine thousand, six hundred and eighty-eight (379,388) trials. However, a brute force password attack is more complicated than that because, as described on page 15 of the pending application, a password may, in principle, contain five (5) or four (4) or three (3) or two (2) or even just one (1) character. Considering the possibility that passwords might contain only four (4) or five (5) characters increases the number of trials required for a brute force password attack to four-hundred and five thousand (405,000). Clearly, manually trying four-hundred and five thousand (405,000) password is impossible. Moreover, for all practical purposes trying four-hundred and five thousand (405,000) passwords is also impossible for an automatic apparatus. If such an apparatus were, on average, able to try one (1) password stored in the pre-boot security controller described in the present application every ten (10) seconds, it would, on average, take more than 1,125 hours, approximately 46.875 days, approximately one and one-half (1½) months to obtain a single password.

The preceding comparison of the number of trials required for a brute force password attack irrefutably demonstrates that, in

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

comparison with the invention disclosed in the present application, due to the Lewis patent's "alarm mode" at best the invention disclosed there provides virtually no security. However, even if a thief were to ignore the Lewis patent's alarm mode or if the alarm mode were to be omitted from device protected by the invention of the Lewis patent, for reasons explained in greater detail below and in the attached "Declaration of Brian Oh"⁶ the invention of the Lewis patent would still provide virtually no security.

On May 4, 1999, United States Patent no. 5,900,014 entitled "External Means of Overriding and Controlling Cacheability Attribute of Selected CPU Accesses to Monitor Instruction and Data Streams" issued which in its abstract declares:

[a]n in-circuit emulator (ICE), which is used for debugging purposes, monitors addresses read by and written to a CPU. If an address which is of interest for debugging purposes is detected by the ICE, then the ICE issues a trigger signal. The trigger signal causes the external trigger state machine to designate the cache line associated with the detected address as a non-cacheable operation (i.e., to override the cacheability attribute). Thus, the data associated with the cache line is written out to the main memory module where the data can be observed by an ICE, rather than to an internal cache memory location where the data would be invisible to an ICE. (Emphasis supplied.)

Paragraph 16 in the attached "Declaration of Brian Oh" irrefutably establishes that "if an ICE, . . . , were coupled to

⁶ The "Declaration of Brian Oh" is hereby incorporated by reference as though fully set forth here.

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

the microcomputer 10 disclosed in the Lewis patent, the ICE could be used to read out the 'predetermined primary security code stored in PROM 34'" keystroke by keystroke during password entry.

Based upon the "Declaration of Brian Oh," the security system disclosed in the Lewis patent may be analogized to a safe having a combination lock which a safecracker, using a stethoscope, can hear operating as he rotates the safe's dial. As is well known, a safe equipped with such a lock truly provides no deterrence to a skilled safecracker with sufficient time to determine the safe's combination.

However, one difference between a safe and an electronic device such as a laptop or notebook computer is readily apparent. Unless a safecracker knows what is in the safe, he is unaware of the value of what he may steal after opening it. That is, when a safecracker opens a safe's door, he may find it empty or full of worthless documents. However, a thief stealing a laptop or notebook computer can assess in advance the value of what he is taking. Thus, as is readily apparent, equipping a laptop or notebook computer with an easily compromised security system such as that disclosed in the Lewis patent provides virtually no deterrence against theft. Consequently, because the "Declaration of Brian Oh" proves that the "predetermined primary security code stored in PROM 34," i.e. the password, can be easily read using an

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

ICE, the Lewis patent is a failed attempt to obtain that reference's desired property of theft deterrence.

Because, as established in the preceding paragraphs and in the "Declaration of Brian Oh," the Lewis patent fails to provide theft deterrence, applying the controlling authority of Chester, Motorola and Rockwell cited above the Lewis patent by itself could not render the apparatus encompassed by the pending claims obvious. Furthermore, applying the holdings of In re Gurley, In re Sponnoble and In re Caldwell cited above, the Lewis patent's failure to provide theft deterrence actually discourages a person of ordinary skill from following the path set out in that reference. Moreover, the Lewis patent "teaches away if it leaves the impression that the product would not have the property sought by the applicant." In re Gurley supra citing In re Caldwell. Paraphrasing the Supreme Court's decision in Adams, that in 1986 Lewis may have been able to convince a United States patent examiner to issue a patent on his device has little significance in the light of the foregoing.

Considering now the disclosures both of the Lewis patent and of the Sibigtroth, et al. patent as combined in the final rejection of claims, paragraph 41 in the attached Declaration of Brian Oh irrefutably establishes that:

constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action merely makes ascertaining the predetermined primary security code, i.e. predetermined primary

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

password, a two step operation, i.e. first record the addresses in the memory 13 [using an ICE] and then obtain from the memory 13 the data stored at those addresses, rather than a one step operation.

Since paragraph 41 in the "Declaration of Brian Oh" proves that using an ICE the primary security code, i.e. predetermined primary password, can be easily read in a two (2) step operation from the microcomputer 10 of the Lewis patent when constructed in the method of the Sibigtroth, et al. patent with passwords being stored in the memory 13 and the microcomputer 10 operating in the "secure mode" described in the Sibigtroth, et al. patent, the combined disclosures of the Lewis and Sibigtroth, et al. patents also constitute a failed attempt to obtain the desired property of theft deterrence.

Once again analogizing the combined disclosures of the Lewis and Sibigtroth, et al. patents to a safe, the combined disclosures don't produce a soundproof safe. Instead, now the safecracker must first record sounds made by the safe's lock while rotating the safe's dial. Then, after recording the safe's sounds, the safecracker by analyzing the recorded sounds is able to determine the safe's combination. A safe that may be cracked by recording the sounds of its lock provides no more deterrent to a skilled safecracker than one which can be cracked using only a stethoscope.

Thus it is clear, for the reasons set forth in the preceding paragraphs, the combined disclosures of the Lewis and Sibigtroth,

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

et al. patents teach nothing which markedly increases the theft deterrence provided the Lewis patent alone. Since a combination of the disclosures of the Lewis and Sibigtroth, et al. patents fails to provide the desired property of theft deterrence alleged for the Lewis patent, the controlling legal authority as applied above to the Lewis patent alone is fully and completely applicable to the combined disclosures of the Lewis and Sibigtroth, et al. patents. Therefore, the disclosures of the Lewis and Sibigtroth, et al. patents as combined in the final rejection of claims, either by themselves or even when combined with the Chao patent or with the Thandiwe patent:

1. are nothing more than a failed attempt that, under controlling authority, cannot render the apparatus encompassed by the pending claims obvious;
2. actually discourage a person of ordinary skill from following the path set out in the combined references; and
3. the combined references teach away from the claimed invention because they leave the impression to one of ordinary skill in the art that their combination lacks the desired property of theft deterrence.

Appl. No. 09/429,174
Response Dated June 1, 2004
Appeal of Office Action dated January 14, 2004

Conclusion

The invention encompassed by independent claims 1 and 10 together with all other claims depending therefrom locates securely and inaccessible entirely within a single integrated circuit, both:

1. storage for the user password; and
2. the digital logic circuit that compares the stored user password with a password received by the integrated circuit.

Storing both the user password and the digital logic circuit within a single integrated circuit prevents accessing the user password by any technique other than, perhaps, discarding or destroying the integrated circuit. Thus, the invention encompassed by the claims pending in this patent application truly provides the theft deterrence sought by the failed attempts both of the Lewis patent alone, and of the Lewis and Sibigtroth, et al. patents as combined in the January 14, 2004, Office Action's final rejection of claims.

For the various reasons set forth in greater detail above, Appellants respectfully submit that:

1. independent claims 1 and 10, together will claims 2-9 and 11-18 depending therefrom, traverse rejection under 35 U.S.C. § 103(a) for obviousness based upon a combination of the Lewis and Sibigtroth, et al. patents, or upon those two (2) references combined with yet another reference because:

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

- a. the references as combined in the January 14, 2004, Office Action fail to produce the structure encompassed by independent claims 1 and 10;
 - b. there truly exists no motivation to combine the Lewis and Sibigtroth, et al. patents other than pending independent claims 1 and 10; and
 - c. applying controlling authority, the failure of the combined references to produce theft deterrence:
 - i. mandates that independent claims 1 and 10 are patentably non-obvious;
 - ii. actually discourages a person of ordinary skill from following the path set out in the combined references; and
 - iii. teaches away from the claimed invention because they leave the impression to one of ordinary skill in the art that their combination lacks the desired property of theft deterrence.
2. dependent claims 4 and 13 independently traverse rejection under 35 U.S.C. § 103(a) for obviousness based upon a combination of the Lewis and Sibigtroth, et al. patents because the combined references fail to disclose or to suggest the "keypad interface" as that phrase is used in claims 4 and 13 and elsewhere in the pending application;

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

3. dependent claims 7 and 16 independently traverse rejection under 35 U.S.C. § 103(a) for obviousness based upon a combination of the Lewis and Sibigtroth, et al. patents because the combined references fail to disclose or to suggest the "state machine" as that phrase is used in claims 7 and 16 and elsewhere in the pending application;
4. dependent claims 8 and 17 independently traverse rejection under 35 U.S.C. § 103(a) for obviousness based upon a combination of the Lewis and Sibigtroth, et al. patents because the combined references fail to disclose or to suggest providing "an output signal which indicates existence of the security operating mode" as used in claims 8 and 17 and elsewhere in the pending application;
and
5. dependent claims 6 and 15 independently traverse rejection under 35 U.S.C. § 103(a) for obviousness based upon a combination of the Lewis, Sibigtroth, et al. and Chao patents because the combined references fail to disclose or to suggest providing an operating mode in which data about pressings of a keypad are preserved as encompassed by claims 6 and 15 and elsewhere in the pending application.

Appl. No. 09/429,174

Response Dated June 1, 2004

Appeal of Office Action dated January 14, 2004

For the reasons enumerated in 1-5 above, Appellants respectfully request that the rejection of claims in the January 14, 2004, Office Action be overturned, and claims 1-18 now pending in this patent application be declared patentable.

Respectfully submitted


Donald E. Schreiber
Reg. No. 29,435

Dated: 1 June, 2004

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Appellants

Appl. No. 09/429,174
Response Dated May 31, 2004
Appeal of Office Action dated January 14, 2004

APPENDIX I
CLAIMS

Claim 1. An integrated circuit pre-boot security controller adapted for inclusion in an electronic device that includes both a digital computer and a power subsystem for energizing operation of the digital computer, the pre-boot security controller receiving 5 electrical power even though the power subsystem is not energizing operation of the digital computer and being adapted for enabling the power subsystem to energize operation of the digital computer upon receiving a pre-recorded user password by the pre-boot security controller, the integrated circuit pre-boot security 10 controller comprising:

a non-volatile password memory that stores at least one user password;

15 a password input circuit for receiving a password that is to be compared with any user passwords recorded in said password memory;

a digital logic circuit for comparing the password received by said password input circuit with any user passwords recorded in said password memory if the pre-boot security controller is in a security operating mode; and

20 an output circuit that is coupled to said digital logic circuit for transmitting an output signal to the power subsystem that enables the power subsystem to energize operation of the

Appl. No. 09/429,174
Response Dated May 31, 2004
Appeal of Office Action dated January 14, 2004

digital computer if the password received by said password input circuit matches a user password recorded in said password memory.

Claim 2. The pre-boot security controller of claim 1 wherein said password memory is electronically rewritable.

Claim 3. The pre-boot security controller of claim 1 wherein said password memory separately records at least one user password and at least one supervisor password.

Claim 4. The pre-boot security controller of claim 1 wherein said password input circuit is a keypad interface that is adapted to be coupled to a security keypad for receiving the password that a user of the electronic device enters using the security keypad for comparison with user passwords recorded in said password memory.

Claim 5. The pre-boot security controller of claim 4 wherein, when in a password entry mode, the keypad interface may also receive from the security keypad user passwords that the digital logic circuit records in said password memory.

Claim 6. The pre-boot security controller of claim 4 wherein upon receiving a password by said password input circuit which matches a user password recorded in said password memory, the pre-boot

Appl. No. 09/429,174
Response Dated May 31, 2004
Appeal of Office Action dated January 14, 2004

security controller transitions from the security operating mode to
5 an application operating mode in which the pre-boot security controller preserves data about pressings of the security keypad.

Claim 7. The pre-boot security controller of claim 1 wherein said digital logic circuit is a state machine.

Claim 8. The pre-boot security controller of claim 1 wherein said output circuit also provides an output signal which indicates existence of the security operating mode.

Claim 9. The pre-boot security controller of claim 1 further comprising a System Management Bus ("SMBus") interface adapted to exchange signals with a SMBus included in the electronic device, said SMBus interface enabling the pre-boot security controller to
5 receive user passwords for storage in said password memory.

Claim 10. An electronic device comprising:

a digital computer;

a power subsystem for energizing operation of said digital computer; and

5 a pre-boot security controller that receives electrical power even though said power subsystem is not energizing operation of said digital computer and that is coupled to said power subsystem

Appl. No. 09/429,174
Response Dated May 31, 2004
Appeal of Office Action dated January 14, 2004

for enabling said power subsystem to energize operation of said digital computer upon receiving a pre-recorded user password by
10 said pre-boot security controller, said pre-boot security controller including:

an integrated circuit that includes:

a non-volatile password memory that stores at least one user password;

15 a password input circuit for receiving a password that is to be compared with any user passwords recorded in said password memory;

20 a digital logic circuit for comparing the password received by said password input circuit with any user passwords recorded in said password memory if the pre-boot security controller is in a security operating mode; and

25 an output circuit that is coupled to said digital logic circuit for transmitting an output signal to said power subsystem that enables said power subsystem to energize operation of said digital computer if the password received by said password input circuit matches a user password recorded in said password memory.

Appl. No. 09/429,174
Response Dated May 31, 2004
Appeal of Office Action dated January 14, 2004

Claim 11. The electronic device of claim 10 wherein said password memory included in said pre-boot security controller is electronically rewritable.

Claim 12. The electronic device of claim 10 wherein said password memory included in said pre-boot security controller separately records at least one user password and at least one supervisor password.

Claim 13. The electronic device of claim 10 wherein said password input circuit included in said pre-boot security controller is a keypad interface, the electronic device further comprising a security keypad that is coupled to the keypad interface to transmit thereto for comparison with user passwords recorded in said password memory the password that a user of the electronic device enters using the security keypad.

Claim 14. The electronic device of claim 13 wherein the keypad interface of said pre-boot security controller, when said pre-boot security controller is in a password entry mode, may also receive from the security keypad user passwords that the digital logic circuit records in said password memory.

Appl. No. 09/429,174

Response Dated May 31, 2004

Appeal of Office Action dated January 14, 2004

Claim 15. The electronic device of claim 13 wherein said pre-boot security controller, upon receiving a password by said password input circuit which matches a user password recorded in said password memory, transitions from the security operating mode to a
5 application operating mode in which the pre-boot security controller preserves data about pressings of the security keypad.

Claim 16. The electronic device of claim 10 wherein said digital logic circuit included in said pre-boot security controller is a state machine.

Claim 17. The electronic device of claim 10 wherein said output circuit of said pre-boot security controller also provides an output signal which indicates existence of the security operating mode, the electronic device further comprising a status output
5 subsystem which receives the output signal and presents a user of the electronic device with a perceptible indication that the security operating mode exists.

Claim 18. The electronic device of claim 10 wherein said pre-boot security controller further includes a SMBus interface, the electronic device further comprising a SMBus host that is coupled by a SMBus to the SMBus interface thereby enabling a computer

Appl. No. 09/429,174

Response Dated May 31, 2004

Appeal of Office Action dated January 14, 2004

- 5 program executed by said digital computer to record user passwords into said password memory via the SMBus.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No. : 09/429,174 Confirmation No. (None)
Applicants : Jung-Chih Huang, et al.
Filed : October 28, 1999
Title : PRE-BOOT SECURITY CONTROLLER
TC/A.U. : 2134
Examiner : Christopher J. Brown

Docket No. : 2139
Customer No.: 23320

DECLARATION OF BRIAN OH

I, BRIAN OH declare that:

1. I am 38 years old and reside at 273 Saratoga Avenue, Santa Clara, California 95050.
2. In 1987, Chun-Buk National University, in Korea, granted me a Bachelors of Science degree in Electronics Engineering.
3. From January 1987, until December 1992, I was employed by Daewoo Telecom, Ltd. in Seoul, Korea as a Hardware Engineer designing main boards for computers which used Intel x86 microprocessors.
4. From January 1993, until August 1995, I was employed by Daewoo Telecom, Ltd. in Santa Clara, California as a Hardware Engineer designing a sound card and docking system for notebook computers which used Intel x86 microprocessors.
5. From September 1995, until March 1997, I was employed by ACC Micro of Santa Clara, California as a Senior System Engineer debugging chipsets for personal computers and providing customer support, and designing a PCMCIA ATA flash controller.

6. From April 1997, until February 1998, I was employed by Trident Microsystems of Mountain View, California as a Senior Application Engineer in a multimedia marketing group debugging integrated circuits and providing customer support.

7. From March 1998 until the present I have been employed by O₂ Micro, Inc., the assignee of the present patent application, as a Senior Application Engineer designing integrated circuits for a CardBus Controller and for Universal Serial Bus ("USB") products, debugging prototype integrated circuits, | and providing customer support.

8. I am a joint inventor with Jung-Chih Huang, Yishao Max Huang, Sterling Du and Aaron Reynoso of the invention disclosed and claimed in the present patent application, and am a co-applicant with them for this patent application.

9. I have reviewed:

- a. the Office Action that issued for this patent application on January 14, 2004;
- b. the references cited in the January 14, 2004, Office Action; and
- c. a response to a prior Office Action for this patent application which was received by the United States Patent and Trademark Office ("USPTO") on October 17, 2003.

10. Based upon my review of the January 14, 2004, Office Action, it appears that there exists a lack of appreciation for the structure and operation of the present invention in comparison with

the references applied in rejecting the patent application's claims.

11. This patent application's invention is:

an integrated circuit pre-boot security controller that includes a non-volatile password memory for storing at least one user password. A password input circuit, included in the pre-boot security controller, receives a password for comparison with any user passwords recorded in the password memory. If the pre-boot security controller is in a security operating mode, a digital logic circuit, also included in the pre-boot security controller, compares the received password with any user passwords recorded in the password memory. If the password received by the password input circuit matches a user password recorded in the password memory, an output circuit of the pre-boot security controller, that is coupled to the digital logic circuit, transmits an output signal to a power subsystem to enable energizing operation of a digital computer.

12. The January 14, 2004, Office Action rejects pending claims 1-18 based upon combinations of United States Patent no. 5,251,304 entitled "Integrated Circuit Microcontroller With On-Chip Memory and External Bus Interface and Programmable Mechanism for Securing the Contents of On-Chip Memory" which issued on a patent application filed in the names of James M. Sibigtroth, Michael W. Rhoades, George G. Grimmer, Jr. and Susan W. Longwell ("the Sibigtroth, et al. patent") either:

- a. with United States Patent no. 4,604,708 entitled "Electronic Security System for Electronically Powered Devices" that issued on August 5, 1986, on a patent application filed by Gainer R. Lewis ("the Lewis patent");
- b. with:

- i. the Lewis patent; and
 - ii. United States Patent no. 5,313,639 entitled "Computer With Security Device for Controlling Access Thereto" which issued May 17, 1994, on a patent application filed by George Chao ("the Chao patent"); or
- c. with
- i. the Lewis patent;
 - ii. the Chao patent; and
 - iii. United States Patent no. 5,594,319 entitled "Battery Pack Having Theft Deterrent Circuit" that issued January 14, 1997, on a patent filed by Iilonga P. Thandiwe ("the Thandiwe patent").

13. It is readily apparent, merely from the titles of the Lewis, Chao and Thandiwe patents, that their respective inventions all attempt to provide security for electrically powered devices, i.e. attempt to bar unpermitted use of electrically powered devices.

14. Based upon my analysis of the Lewis, Chao and Thandiwe patents specifically set forth below, it is clear that the inventions respectively disclosed in those patents provide only an illusion of security.

15. Conversely, in comparison with the inventions respectively disclosed in the Lewis, Chao and Thandiwe patents, the invention

disclosed in the present application provides true security for electrically powered devices.

16. For the Lewis patent, if an in-circuit emulator ("ICE"), such as that disclosed in United States Patent No. 5,900,014 entitled "External Means of Overriding and Controlling Cacheability Attribute of Selected CPU Accesses to Monitor Instruction and Data Streams" ("the '014 patent") that issued May 4, 1999, were coupled to the microcomputer 10 disclosed in the Lewis patent, the ICE could be used to read out the "predetermined primary security code stored in PROM 34."¹

17. For the Chao patent, the casing (1) can be easily removed from the disk drive receiving space (40) and replaced by an identical substitute casing which holds a known password in the replacement casing's ROM unit (32).

18. Also for the Chao patent, the casing (1) may be merely removed, and jumpers substituted for the relay unit (331, 341, 351) thereby entirely eliminating any need for entering a password.

19. For the Thandiwe patent, the secure battery system described in the Thandiwe patent can be avoided merely by connecting to the host device 12 a substitute battery pack (10) having a known password stored in its memory 26.

20. Also for the Thandiwe patent, a battery pack entirely lacking the microcontroller circuit 20 and the logic circuit 28 can

¹ See the '014 patent for a more complete description of how an ICE may be used to acquire data that is being accessed by a microprocessor.

be connected to the host device 12 for energizing its operation without any need for entering a password.

21. For the preceding reasons, clearly the security inventions respectively disclosed in of the Lewis, Chao and Thandiwe patents, individually by themselves, can be easily defeated in the simple ways described above, and therefore provide only an illusion of security.

22. The text of the January 14, 2004, Office Action at the bottom of page 4 expressly combines the Sibigtroth, et al. patent with only the Lewis patent stating:

Sibitroth (sic) discloses a controller and memory as part of an integrated circuit (Sibitroth [sic] Col 2 lines 19-25). It would be obvious to one skilled in the art to construct the microcomputer of Lewis in the method of Sibitroth because it is more compact.

23. I am unable to find in the January 14, 2004, Office Action any express combination of the Sibigtroth, et al. patent with:

- a. the Chao patent; or
- b. the Thandiwe patent.

24. The Lewis patent clearly discloses that the microcomputer 10 compares the keyed in security code, i.e. password, keystroke by keystroke with a predetermined primary security code, i.e. predetermined primary password, stored in PROM 34. (Col. 3, lines 50-53)

25. The Sibigtroth, et al. patent discloses a data processing system 10 that includes an integrated circuit package portion 11

and a peripheral portion 12 having an external peripheral device.
(Col. 2, lines 19-22)

26. As described in col. 2 of the Sibigtroth, et al. patent at lines 22-25, the integrated circuit package portion 11 includes:

- a. a memory 13;
- b. a data processor 14;
- c. a decoder 16;
- d. an instruction inhibit circuit 18; and
- e. a programmable security device 20.

27. Attached hereto as Exhibit A is a copy of FIG. 1 of the Sibigtroth, et al. patent that has been annotated with a dashed line that encloses the integrated circuit package portion 11 of the data processing system 10. (Col. 2, lines 26-49)

28. The Abstract of the Sibigtroth, et al. patent discloses that integrated circuit package portion 11 operates in three different modes:

- a. a "secure mode;"
- b. a "single chip mode;" and
- c. an "expanded mode."

29. When the integrated circuit package portion 11 operates in the "secure mode," the data processor 14 with memory 13 within the single integrated circuit package portion 11:

- a. restricts instruction access to memory 13 contained within the integrated circuit package portion 11;
- b. while allowing data accesses to:
 - i. either the internal memory 13; or

ii. to a memory external to the integrated circuit package portion 11. (Abstract)

30. When the integrated circuit package portion 11 operates in the "single chip mode," the data processor 14 accesses both data and instructions strictly from within the integrated circuit package portion 11. (Abstract)

31. When the integrated circuit package portion 11 operates in the "expanded mode," the data processor 14 may access either the internal memory 13 or external memory for both instructions and data. (Abstract)

32. If constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action retains the PROM 34 for storing the predetermined primary security code, i.e. predetermined primary password, then the predetermined primary password may be easily obtained using an ICE as the microcomputer 10 compares the keyed in security code, i.e. password, keystroke by keystroke with the predetermined primary security code, i.e. predetermined primary password, stored in PROM 34. (Col. 3, lines 50-53)

33. Therefore, constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action does not alter the security provided by the invention disclosed in the Lewis patent if the predetermined primary security code, i.e.

predetermined primary password, is stored in the PROM 34 external to the Sibigtroth-style microcomputer 10.

34. Furthermore, if constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action retains the PROM 34 for storing the predetermined primary security code, i.e. predetermined primary password, then it will be no more compact than the disclosure of the Lewis patent.

35. Consequently, constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action is more compact and betters the security provided by the Lewis patent only if the predetermined primary security code, i.e. predetermined primary password, were stored in the memory 13 of the integrated circuit package portion 11.

36. In the secure mode of operation of the Sibigtroth, et al. patent's integrated circuit package portion 11, instruction read cycles performed by the data processor 14 are confined to the data processor (sic)² as in the single chip mode, whereas data reads and writes initiated by the data processor 14 can be made either internal or external to the data processor 14 as in the expanded mode of operation. The secure mode of operation provided by the Sibigtroth, et al. patent is an effective and economical solution

² It appears that this text is incorrect, and should correctly read "confined to the integrated circuit package portion 11."

to isolate instruction information of a data processor while
allowing the data processor to read or write non-proprietary data
external to the data processor.

*

*

*

However, regardless of the variety of operations considered permissible within a single chip or expanded mode of operation, the functionality of the secure mode insures that memory 13 may not be read or modified by unauthorized sources external to the single integrated circuit package. (Col. 4 lines 38-60)

37. Referring now to Exhibit A, i.e. FIG. 1 of the Sibigtroth, et al. patent, it is readily apparent that comparing the keyed in security code, i.e. password, keystroke by keystroke with a predetermined primary security code, i.e. predetermined primary password, as required by the Lewis patent using the Sibigtroth, et al. patent's data processing system 10 requires that the peripheral portion 12 must provide the keyed in security code to the integrated circuit package portion 11.

38. Referring again to Exhibit A, it is also readily apparent that even when the integrated circuit package portion 11 operates either in its "secure mode" or in its "single chip" mode, an ICE connected to the integrated circuit package portion 11 can monitor and record, via the address bus 22 which extends from inside the integrated circuit package portion 11 outside to the peripheral portion 12, all addresses from which the data processor 14 fetches data and instructions from the memory 13.

39. Since col. 3, lines 50-53 of the Lewis patent discloses that the microcomputer 10 compares the keyed in security code, i.e. password, keystroke by keystroke with a predetermined primary security code, if a Sibigroth-style microcomputer 10 stored the Lewis patent's predetermined primary security code, i.e. predetermined primary password, in its memory 13, and if the Sibigroth-style microcomputer 10 were operating in its "secure mode,"³ by monitoring the address bus 22 an ICE connected to the integrated circuit package portion 11 can record all addresses in the memory 13 from which the data processor 14 fetches data and instructions while comparing keystroke by keystroke the keyed in security code, i.e. password, with the predetermined primary security code, i.e. predetermined primary password stored in the memory 13.

40. Using an ICE, having thus monitored and recorded all addresses in the memory 13 from which the data processor 14 fetches data and instructions while comparing keystroke by keystroke the keyed in security code, i.e. password, with the predetermined primary security code, i.e. predetermined primary password, one could then readily ascertain the predetermined primary security code, i.e. predetermined primary password, by operating the integrated circuit package portion 11 in its "expanded mode" and exporting from the integrated circuit package portion 11 to the ICE

³ Note that if the Sibigroth-style microprocessor 10 were operating in its "single chip mode," it could not receive via the data/instruction bus 30 a "keyed in security code."

the data stored in the memory 13 at the address previously monitored and recorded using the ICE.

41. Thus, constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action merely makes ascertaining the predetermined primary security code, i.e. predetermined primary password, a two step operation, i.e. first record the addresses in the memory 13 and then obtain from the memory 13 the data stored at those addresses, rather than a one step operation.

42. Furthermore, constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action and storing the predetermined primary security code, i.e. predetermined primary password, in the memory 13 of the integrated circuit package portion 11 fails to provide non-volatile password storage.

43. Consequently, if one were to construct the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action and were to store the predetermined primary security code, i.e. predetermined primary password, in the memory 13 of the integrated circuit package portion 11, due to a lack of non-volatile storage the predetermined primary security code, i.e. predetermined primary password, would be forever lost if electrical power were removed from the integrated circuit package portion 11.

44. I am unaware of any facts contrary to the facts and opinions contained in this Declaration.

45. I declare under penalty of perjury under the laws of the United States of America that all statements made herein of my own knowledge are true and correct, and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of any patent issuing on the subject application.



Brian Oh

Dated: 2-17, 2004



Oct. 5, 1993

Sheet 1 of 2

5,251,304

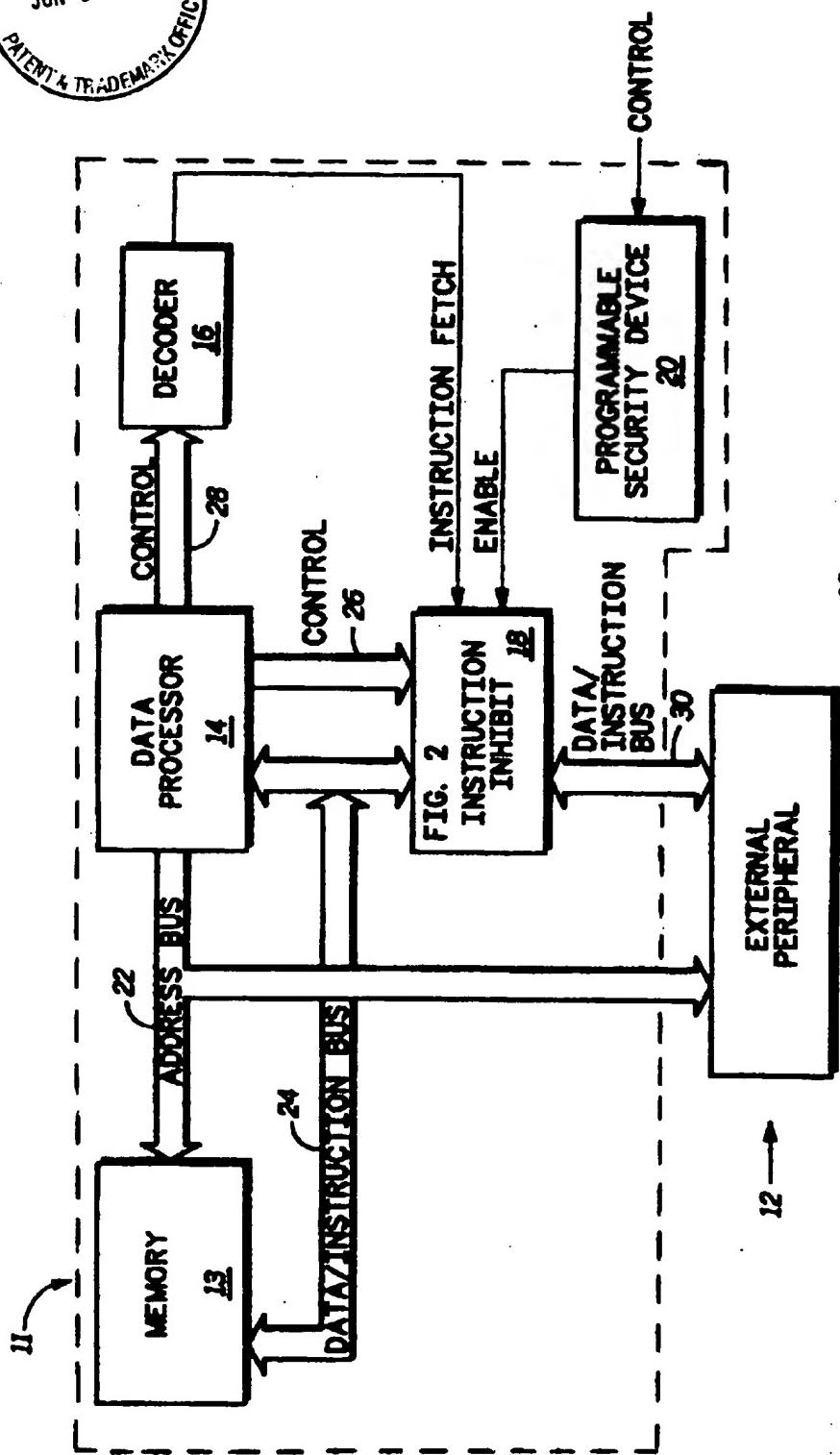


FIG. 1

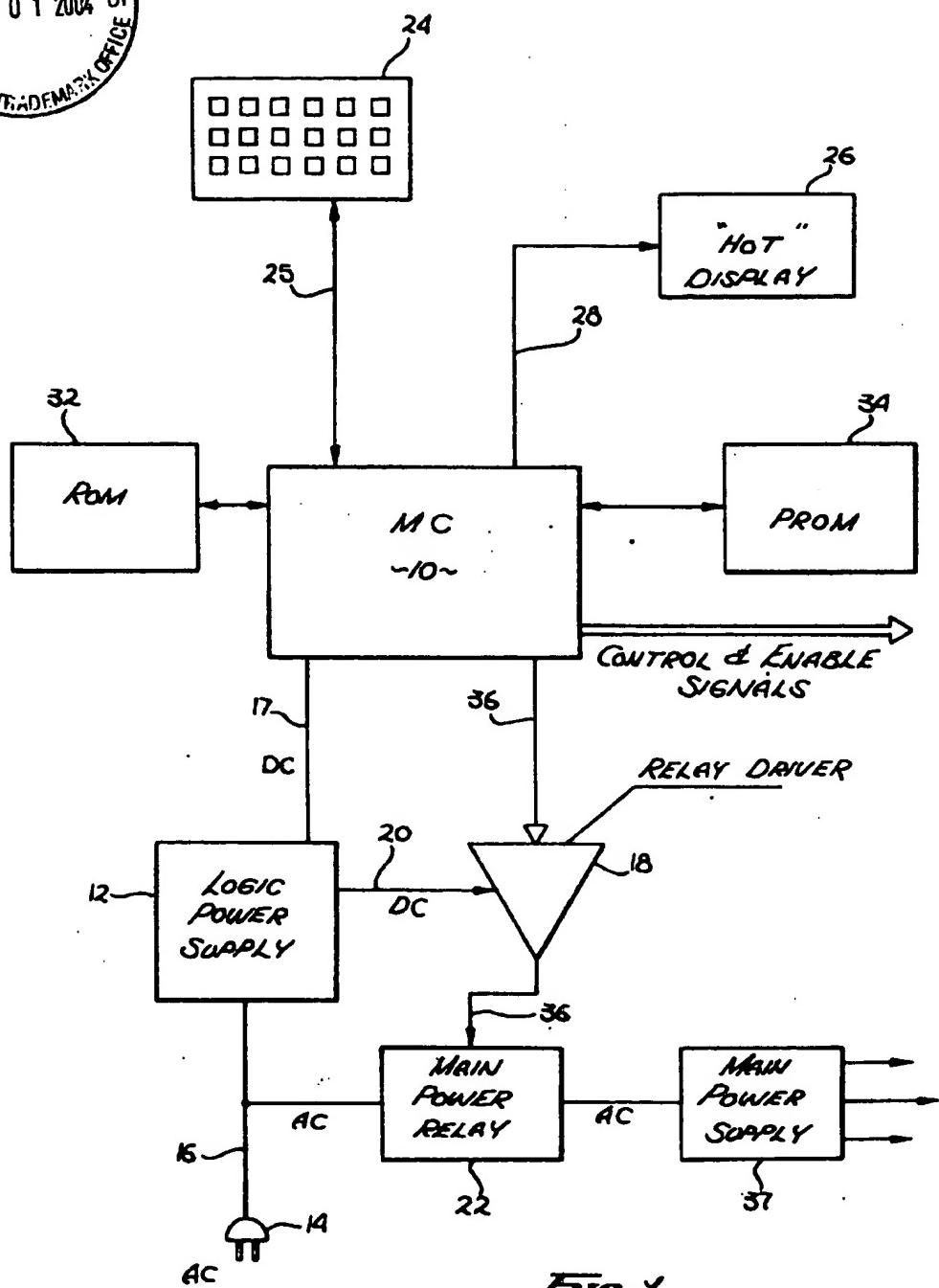


Fig. 2

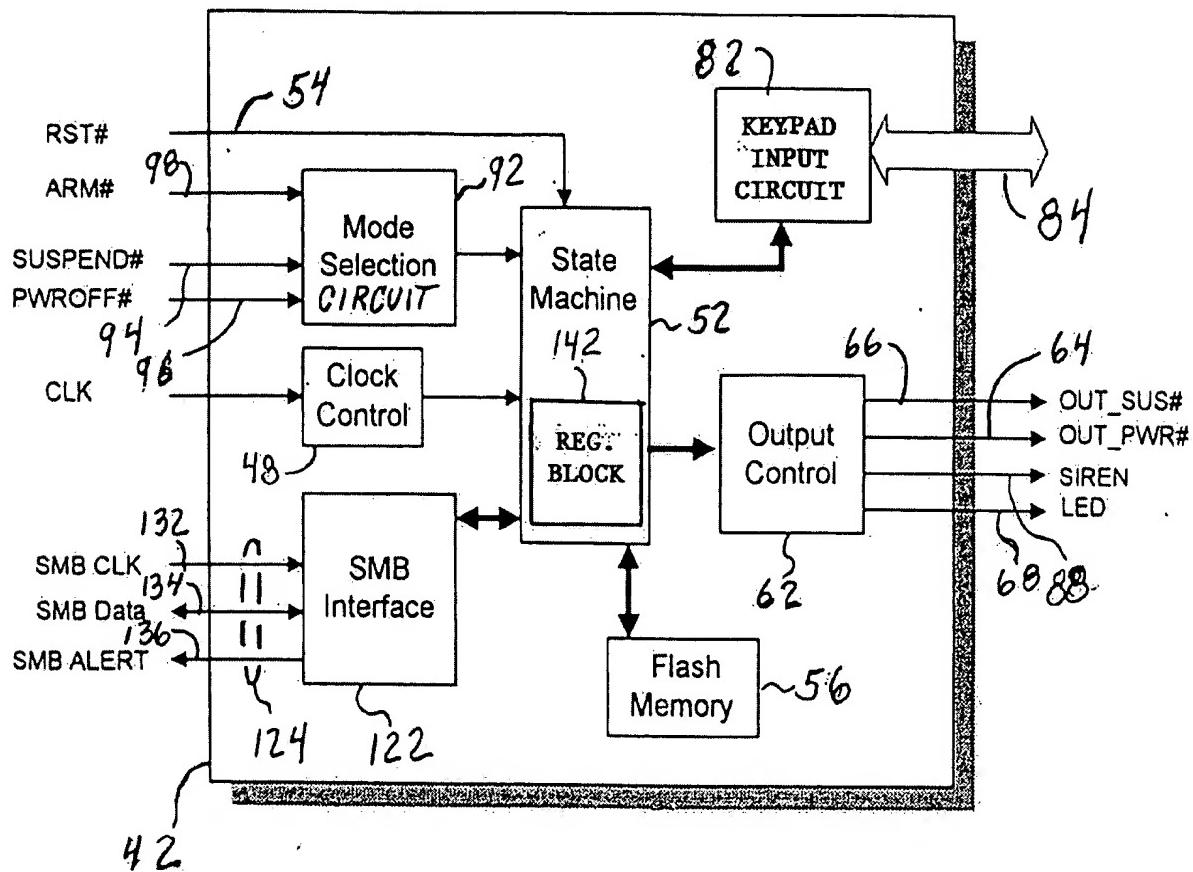


FIG. 2